

100

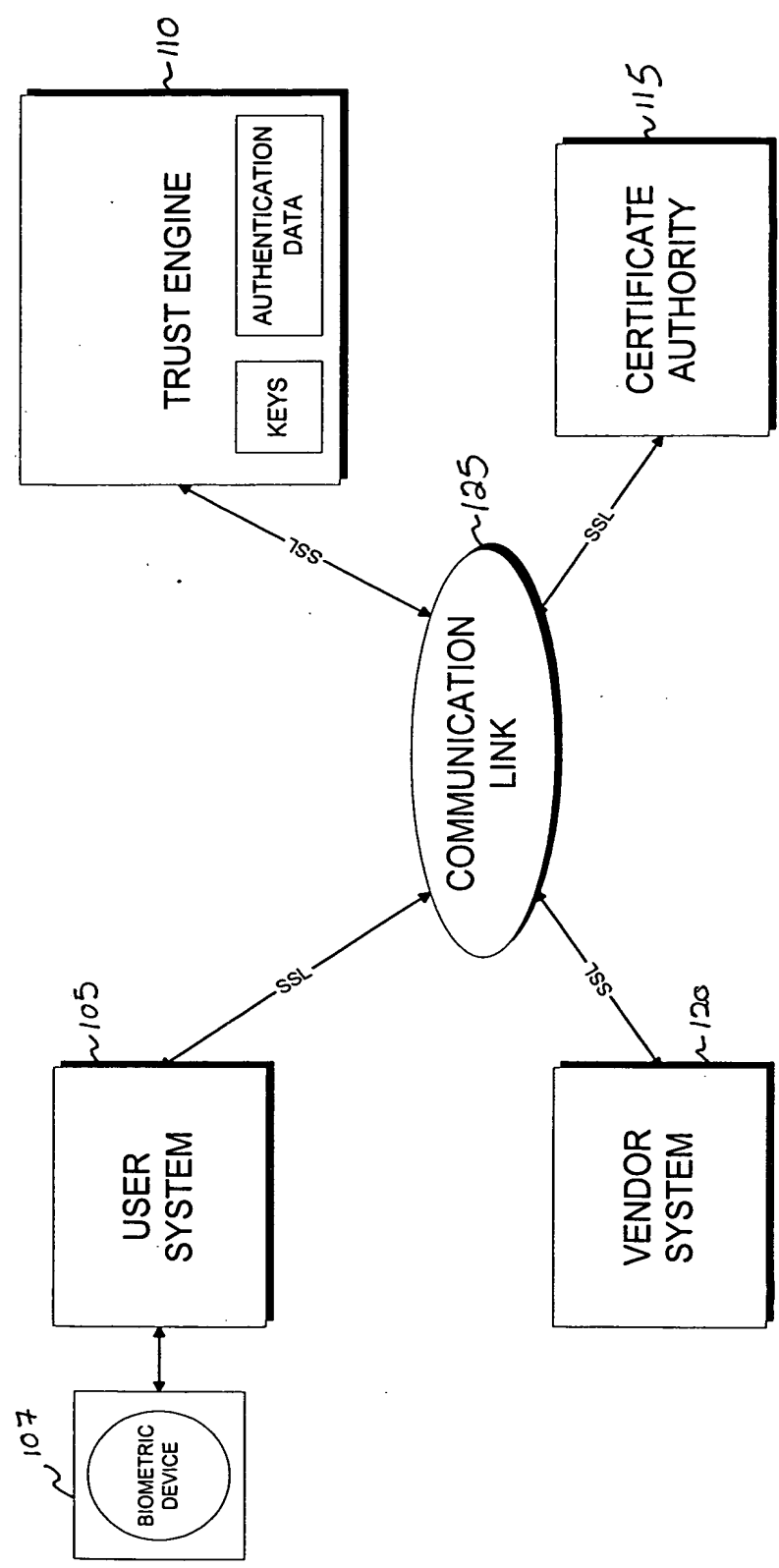


FIG. 1

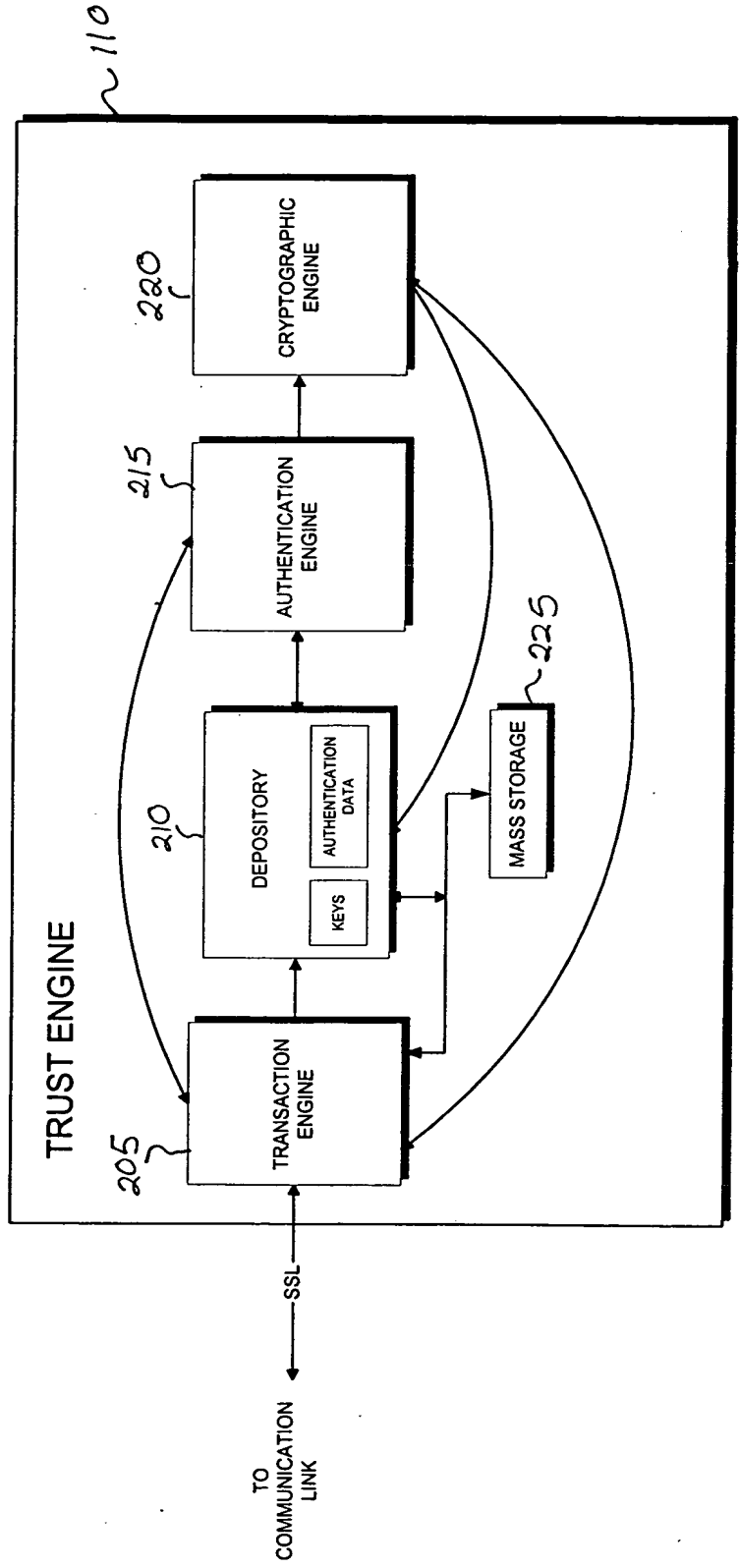


FIG. 2

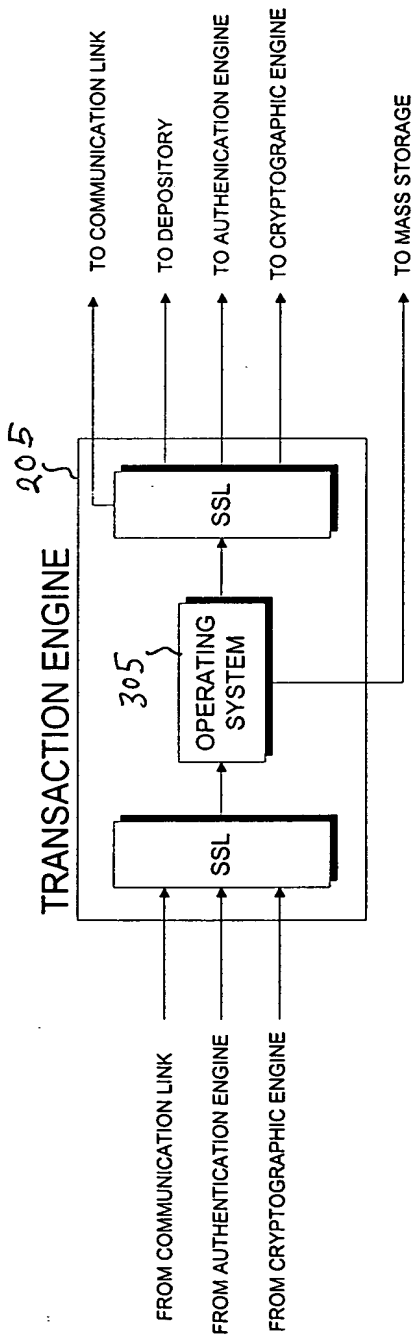


FIG. 3

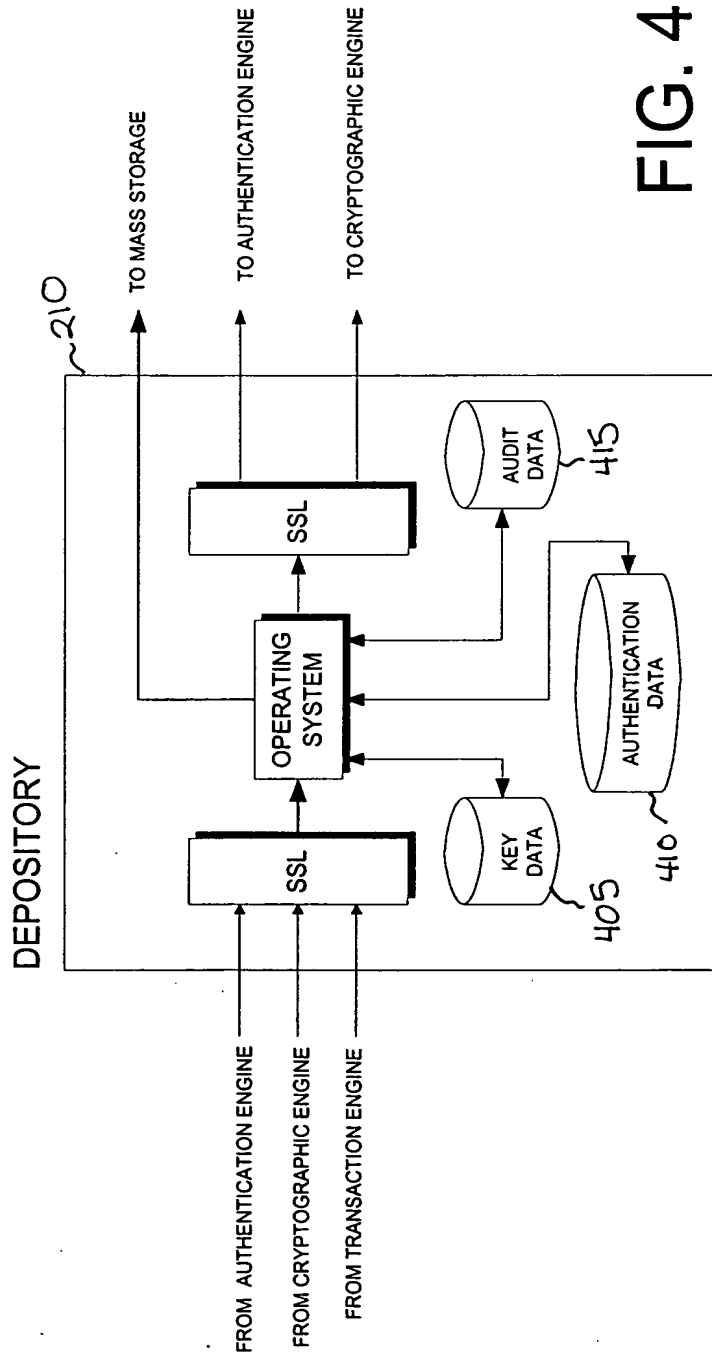


FIG. 4

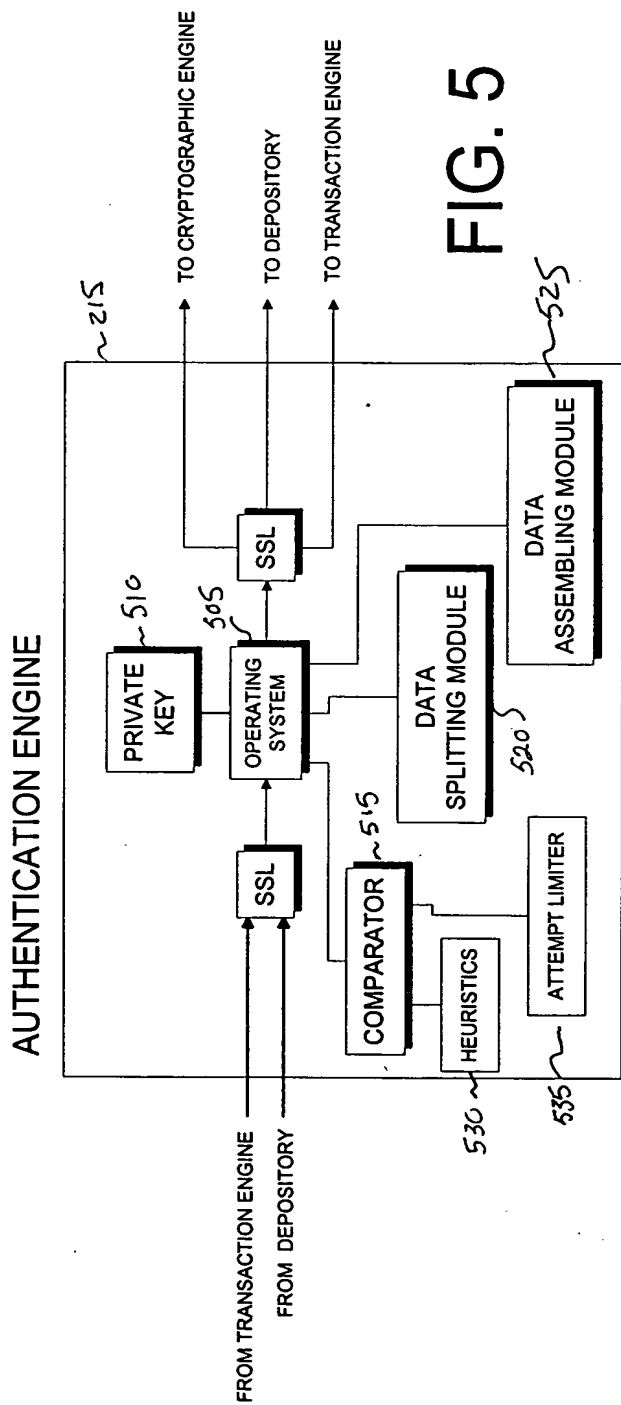


FIG. 5

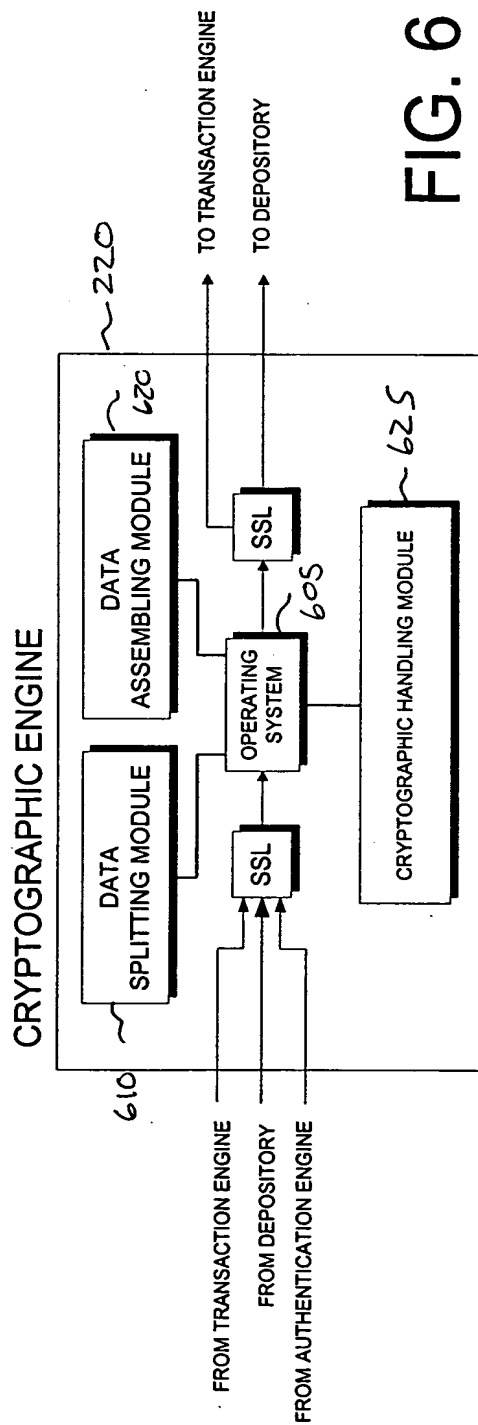


FIG. 6

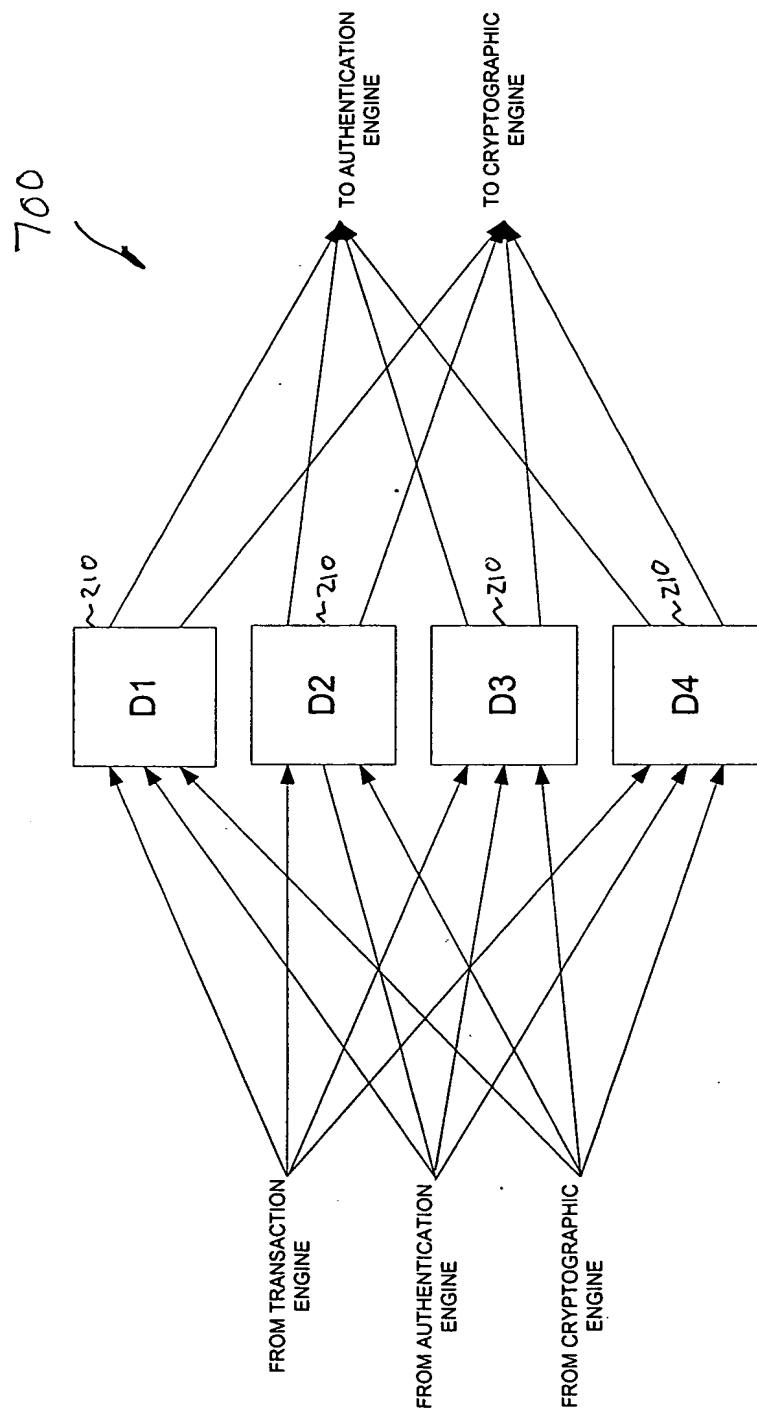
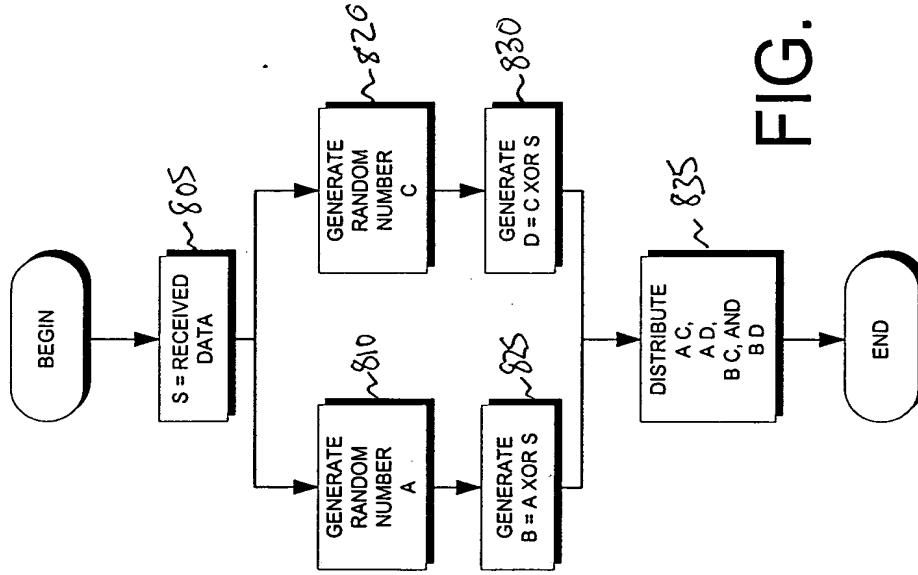


FIG. 7

800  
✓



900  
↙

0000250" 2299960

ENROLLMENT DATA FLOW			
SEND	RECEIVE	SSL	ACTION
905 ~ USER	TRANSACTION ENGINE (TE)	½	TRANSMIT ENROLLMENT AUTHENTICATION DATA (B) AND THE USER ID (UID) ENCRYPTED WITH THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(UID, B))
915 ~ TE	AE	FULL	FORWARD TRANSMISSION
920 ~			AE DECRYPTS AND SPLITS FORWARDED DATA
925 ~ AE	THE X <sup>TH</sup> DEPOSITORY (DX)	FULL	STORE RESPECTIVE PORTION OF DATA
WHEN DIGITAL CERTIFICATE REQUESTED			
930 ~ AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST KEY GENERATION
935 ~			CE GENERATES AND SPLITS KEY
945 ~ CE	TE	FULL	TRANSMIT REQUEST FOR DIGITAL CERTIFICATE
950 ~ TE	CERTIFICATION AUTHORITY (CA)	½	TRANSMIT REQUEST
955 ~ CA	TE	½	TRANSMIT DIGITAL CERTIFICATE
960 ~ TE	USER	½	TRANSMIT DIGITAL CERTIFICATE
	MS	FULL	STORE DIGITAL CERTIFICATE
965 ~ CE	DX	FULL	STORE RESPECTIVE PORTION OF KEY

FIG. 9A

```

graph TD
    970([BEGIN]) --> 972[DETERMINE CERTIFICATE TYPE]
    972 --> 974{DOES USER OWN THIS TYPE OF CERTIFICATE?}
    974 -- Y --> 976[PERFORM ACTION]
    974 -- N --> 978{DOES USER OWN CROSS-CERTIFIED CERTIFICATE?}
    978 -- Y --> 976
    978 -- N --> 980[SELECT CERTIFICATE AUTHORITY THAT ISSUES CERTIFICATE OR CROSS-CERTIFIED CERTIFICATE]
    980 --> 982{DOES USER MEET CURRENT CERTIFICATION AUTHORITY'S AUTHENTICATION REQUIREMENTS?}
    982 -- Y --> 988[UPDATE USER AUTHENTICATION]
    982 -- N --> 986{ARE THERE OTHER CERTIFICATE AUTHORITIES HAVING DIFFERENT AUTHENTICATION REQUIREMENTS?}
    986 -- Y --> 980
    986 -- N --> 988
    988 --> 984[ACQUIRE CERTIFICATE FROM CERTIFICATE AUTHORITY]
    984 --> 976
    976 --> 970
  
```

FIG. 9B

**FIG. 9B**



1000  
↓

# **AUTHENTICATION DATA FLOW**

1005 ~  
1010 ~  
  
1015 ~  
1020 ~  
1025 ~  
1030 ~  
1035 ~  
1040 ~  
1045 ~  
1050 ~  
1055 ~

SEND	RECEIVE	SSL	ACTION
USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE
VENDOR	USER	½	TRANSMIT TRANSACTION ID (TID), AND AUTHENTICATION REQUEST (AR)
			AUTHENTICATION DATA (B') IS GATHERED FROM USER
USER	TE	½	TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B'))
TE	AE	FULL	FORWARD TRANSMISSION
			ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS TID, AR
TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
TE	THE X <sup>TH</sup> DEPOSITORY (DX)	FULL	UID, TID
DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
			AE ASSEMBLES B AND COMPARES TO B'
AE	TE	FULL	TID, THE FILLED IN AR
TE	VENDOR	FULL	TID, YES/NO
TE	USER	½	TID, CONFIRMATION MESSAGE

**FIG. 10**

1100  
↓

0966377-092000

103~  
105~  
110~  
115~  
120~  
125~  
130~  
135~  
140~

SIGNING DATA FLOW			
SEND	RECEIVE	SSL	ACTION
USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS AGREEING ON A DEAL
VENDOR	USER	½	TRANSMIT TRANSACTION IDENTIFICATION NUMBER (TID), AUTHENTICATION REQUEST (AR), AND AGREEMENT OR MESSAGE (M)
			CURRENT AUTHENTICATION DATA (B') AND A HASH OF THE MESSAGE RECEIVED BY THE USER (h(M')) IS GATHERED FROM USER
USER	TE	½	TRANSMIT TID, B', AR, AND h(M') WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(TID, B', h(M')))
TE	AE	FULL	FORWARD TRANSMISSION
			GATHER ENROLLMENT AUTHENTICATION DATA
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS UID, TID, AR, AND A HASH OF THE MESSAGE (h(M)).
TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
TE	THE X <sup>TH</sup> DEPOSITORY (DX)	FULL	UID, TID
DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
			THE ORIGINAL VENDOR MESSAGE IS TRANSMITTED TO THE AE
TE	AE	FULL	TRANSMIT h(M)
			AE ASSEMBLES B, COMPARES TO B' AND COMPARES h(M) TO h(M')
AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST FOR DIGITAL SIGNATURE AND A MESSAGE TO BE SIGNED, FOR EXAMPLE, THE HASHED MESSAGE
AE	DX	FULL	TID, SIGNING UID
DX	CE	FULL	TRANSMIT THE PORTION OF THE CRYPTOGRAPHIC KEY CORRESPONDING TO THE SIGNING PARTY
			CE ASSEMBLES KEY AND SIGNS
CE	AE	FULL	TRANSMIT THE DIGITAL SIGNATURE (S) OF SIGNING PARTY
AE	TE	FULL	TID, THE FILLED IN AR, h(M), AND S
TE	VENDOR	FULL	TID, A RECEIPT = (TID, YES/NO, AND S), AND THE DIGITAL SIGNATURE OF THE TRUSTENGINE, FOR EXAMPLE, A HASH OF THE RECEIPT ENCRYPTED WITH THE TRUSTENGINE'S PRIVATE KEY (Priv_TE(h(RECEIPT))
TE	USER	½	TID, CONFIRMATION MESSAGE

FIG. 11

1200



000260 / 2E99960

1205 ~

1210 ~

1215 ~

1220 ~

1225 ~

1230 ~

1235 ~

1240 ~

1245 ~

1250 ~

ENCRYPTION/DECRYPTION DATA FLOW			
SEND	RECEIVE	SSL	ACTION
DECRYPTION			
			PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SNYC)
			AUTHENTICATE THE USER
AE	CE	FULL	FORWARD PUB_USER(SYNC) TO CE
AE	DX	FULL	UID, TID
DX	CE	FULL	TRANSMIT THE TID AND THE PORTION OF THE PRIVATE KEY AS (PUB_AE(TID, KEY_USER))
			CE ASSEMBLES THE CRYPTOGRAPHIC KEY AND DECRYPTS THE SYNC
CE	AE	FULL	TID, THE FILLED IN AR INCLUDING DECRYPTED SYNC
AE	TE	FULL	FORWARD TO TE
TE	REQUESTING APP/VENDOR	½	TID, YES/NO, SYNC
ENCRYPTION			
REQUESTING APP/VENDOR	TE	½	REQUEST FOR PUBLIC KEY OF USER
TE	MS	FULL	REQUEST DIGITAL CERTIFICATE
MS	TE	FULL	TRANSMIT DIGITAL CERTIFICATE
TE	REQUESTING APP/VENDOR	½	TRANSMIT DIGITAL CERTIFICATE

FIG. 12

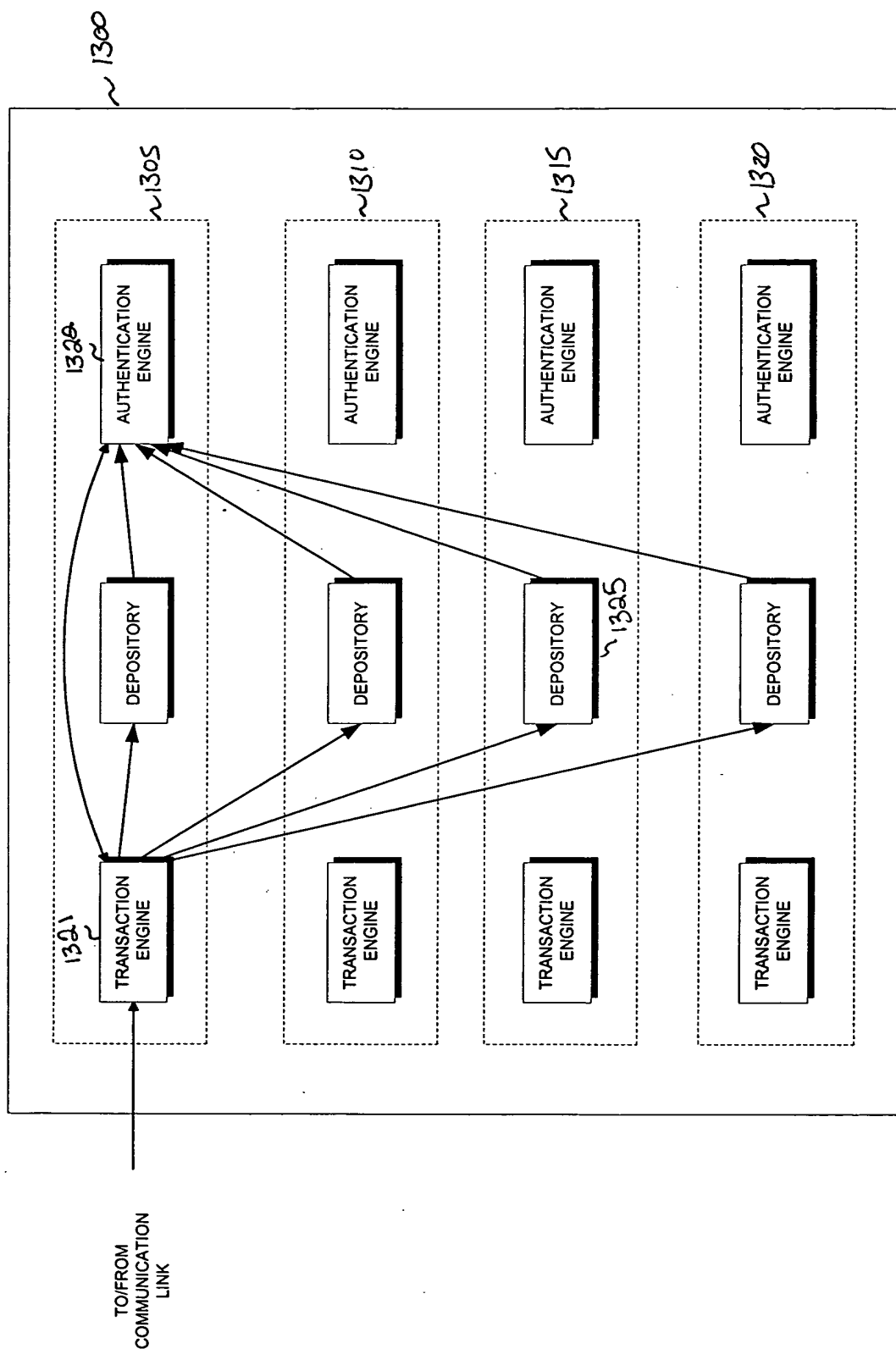


FIG. 13

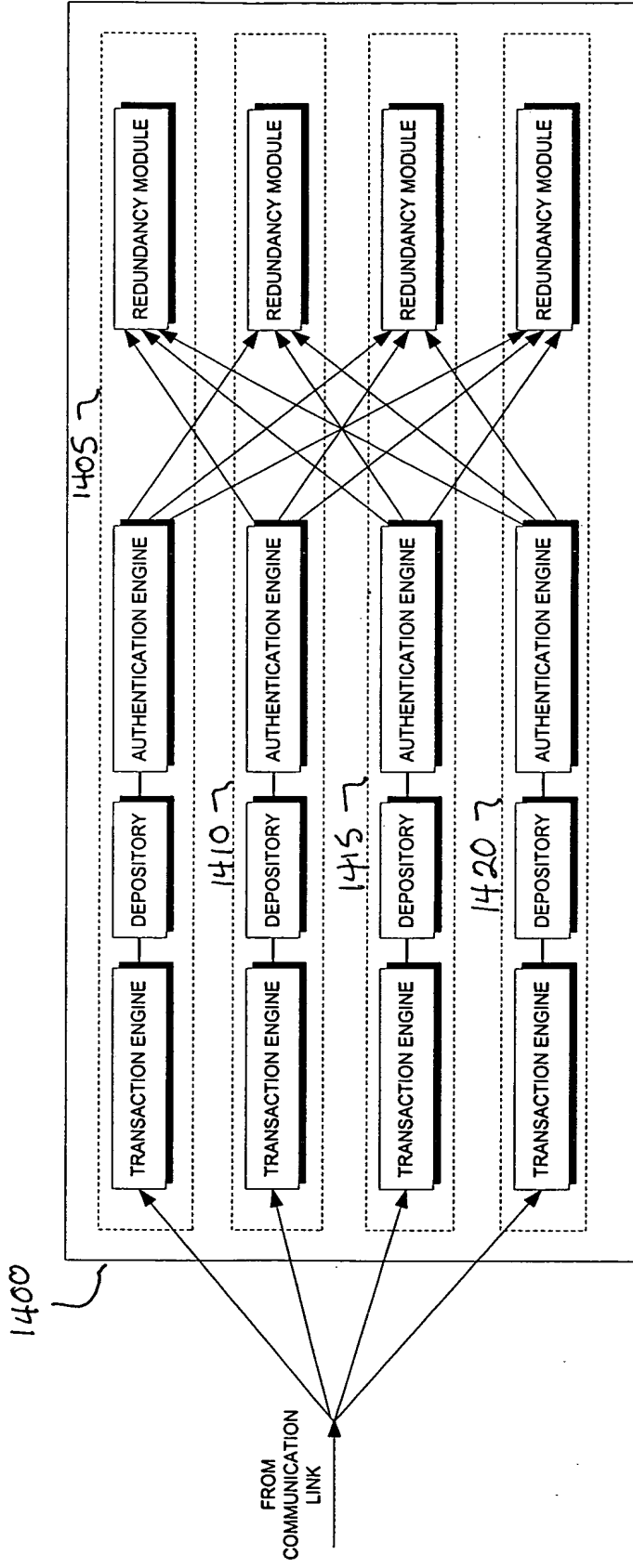
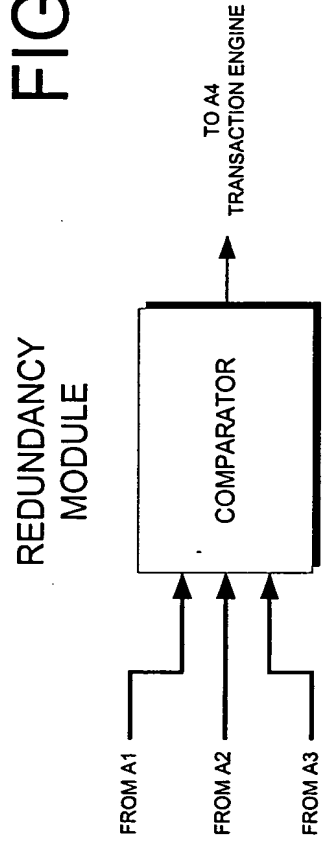
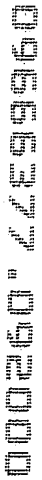


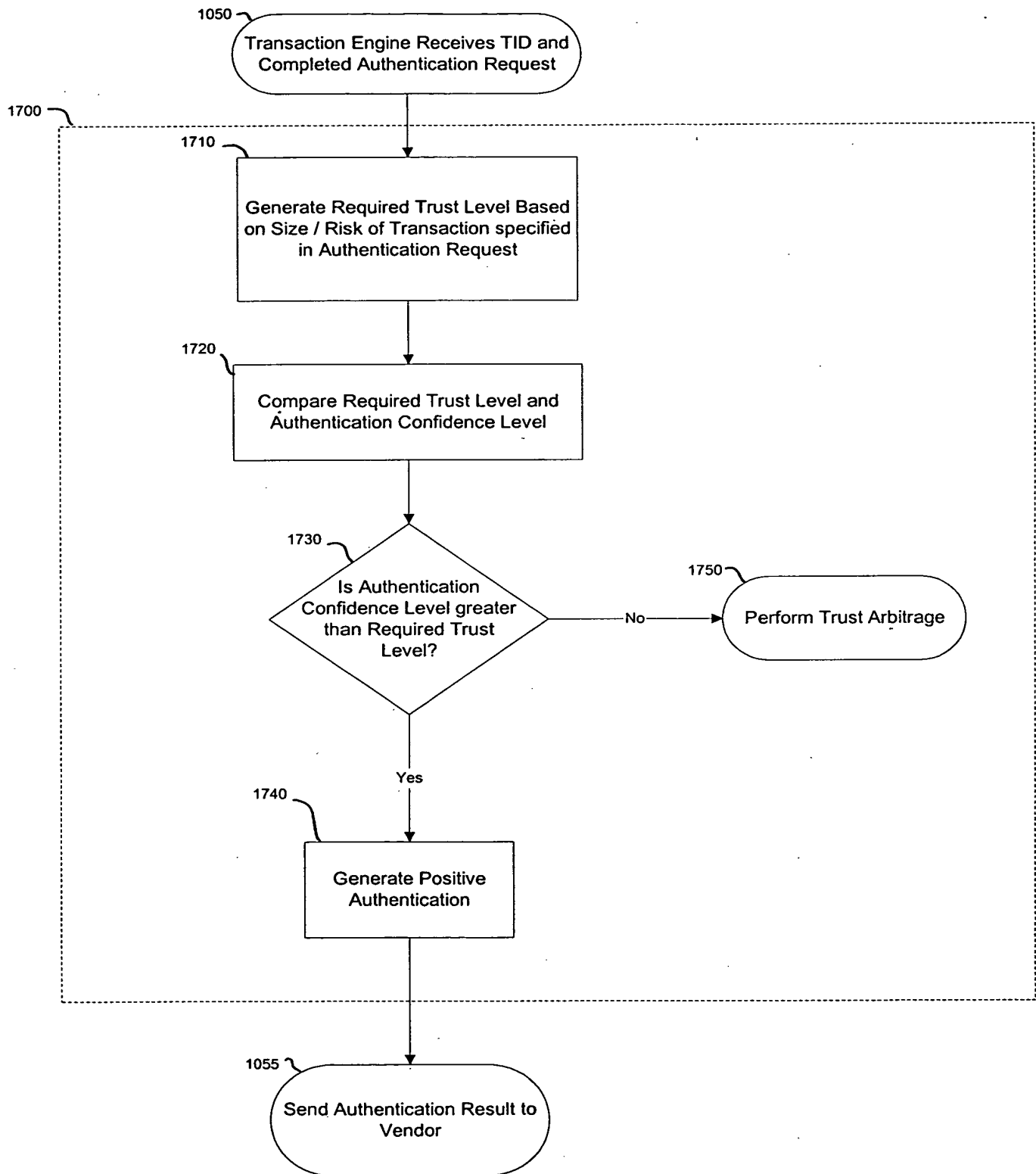
FIG. 14

FIG. 15





# FIGURE 17



000260" 2/299960





# FIGURE 19

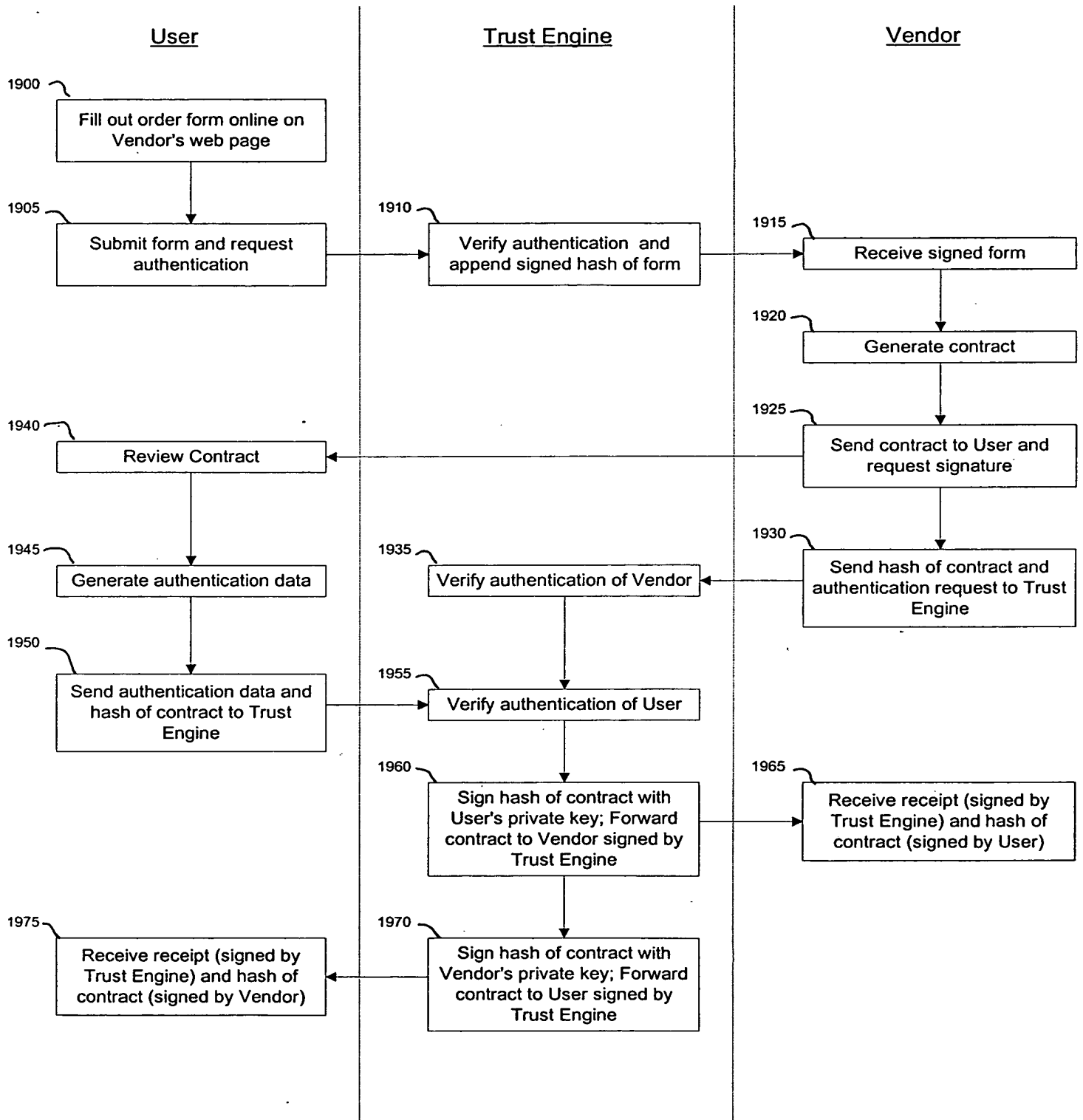
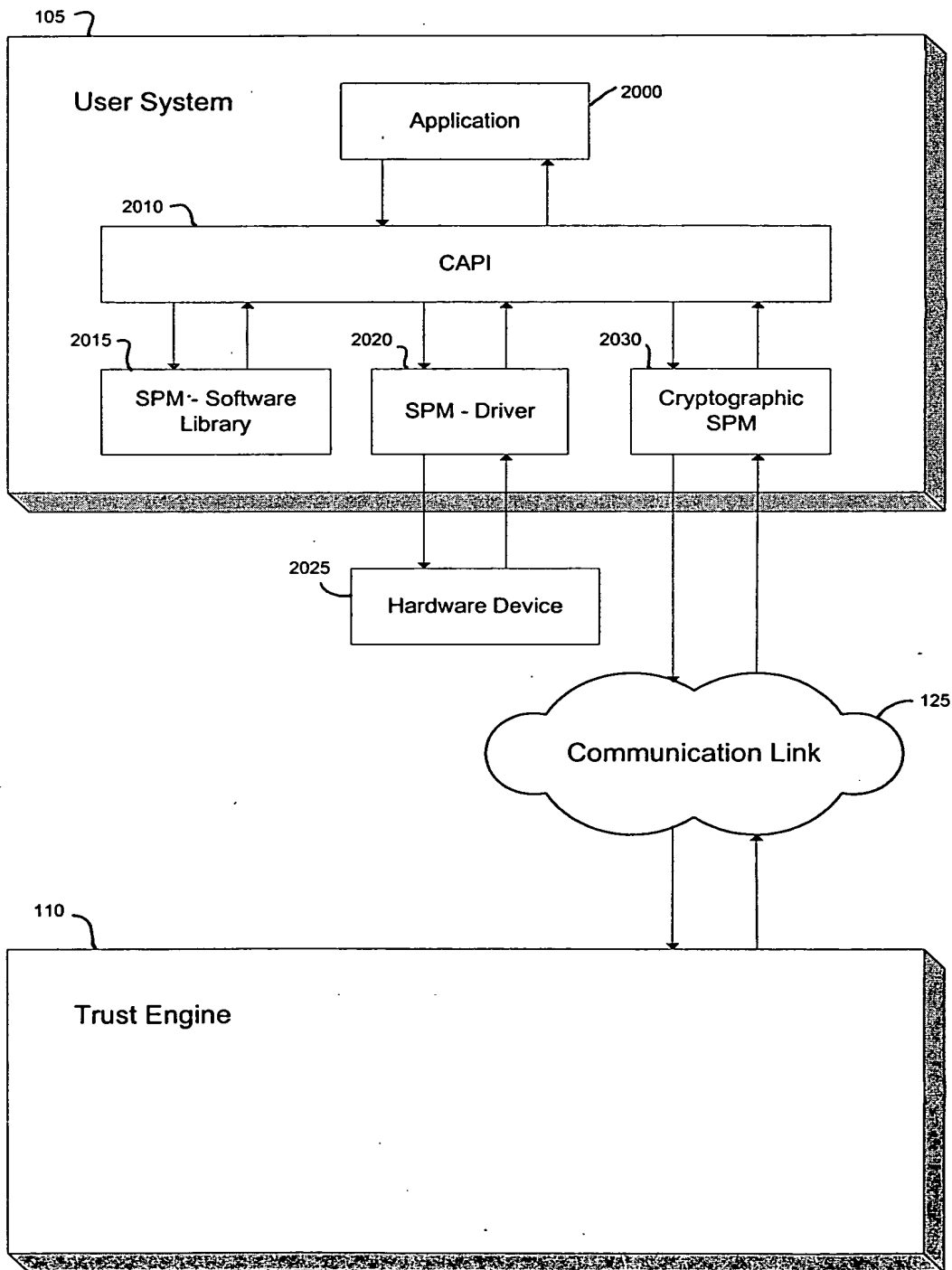


FIGURE 20



000260" / 2E9960